IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: LIANG et al.	Attorney Docket No.: TRNDP009
Application No.: 10/684,330	Examiner: Gee, Jason Kai Yin
Filed: October 9, 2003	Group: 2134
Title: VIRUS MONITOR AND METHODS OF USE THEREOF	Confirmation No.: 9224

CERTIFICATE OF EFS-WEB TRANSMISSION

I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on November 18, 2008.

Signed: /Kathryn Throckmorton/
Kathryn Throckmorton

APPLICANT INITIATED INTERVIEW REQUEST FORM

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Tentative Participants:

1) Steven Chang
2)
3)
4)

Proposed Date of Interview:
Wednesday, November 19, 2008 Proposed Time: **3:15 PM (Eastern Time)**

Type of Interview Requested:

☒ Telephone ☐ Personal ☐ Video Conference

Exhibit to be Shown or Demonstrated: ☐ Yes ☒ No
If yes, provide brief description:

ISSUES TO BE DISCUSSED

Issues (Rej., Obj., etc.)	Claims/ Fig., #s	Prior Art	Discussed	Agreed	Not Agreed
1)Rejection	1	*Ramsey, Douglas, White*	☐	☐	☐
2) Rejection	5	*Ramsey*	☐	☐	☐
3) Rejection	6	*Ramsey*	☐	☐	☐
4) Rejection	10, 17	*Ramsey, Douglas, White*	☐	☐	☐

BRIEF DESCRIPTION OF AGRUMENTS TO BE PRESENTED:

1) Claim 1 has been amended to more clearly recite the claim limitations. The present application teaches a virus sensor operable in a first mode where original data packets continue to their destination after they are copied creating copied data packets which are analyzed for computer viruses. See paragraph [0042]. When the virus sensor detects a virus sensor detects the computer virus, the virus sensor switches to a second mode where original data packets are analyzed and a subset of data packets determined to be infected or suspected of being infected are not returned to the network. See paragraph [0044].

The Ramsey reference does not teach switching over to the second mode from the first mode when a virus is detected. Instead, Ramsey teaches a firewall, intrusion detection system, and virus scanner operable in a number of modes (monitor, ignore) without discussing switching from one mode to another. All of the other cited references also do not discuss switching from one mode to another. Moreover, it is unclear which of these elements (firewall, intrusion detection system, virus scanner) the Examiner has characterized as being analogous to the virus sensor in claim 1.

2) Claim 5 is not disclosed in the cited reference. Although Ramsey teaches employing different protocols for processing information (see col. 10, 9-13), Ramsey does not teach identifying the packet protocol associated with a data packet infected by a computer virus.

3) Claim 6 has been amended to more clearly recite the claim limitations. Although Ramsey teaches employing user-defined rules to determine whether a packet can pass through the firewall (see col. 10, 7-9), Ramsey does not explicitly teach the use of a packet protocol identifier to select packets.

4) Claims 10 and 17 have been amended to more clearly recite the claim limitations. Applicants have amended claims 10 and 17 to clarify that monitoring in an inline mode occurs in response to determining that at least one of the copied packets is infected or suspected of being infected with the computer virus. As discussed above in issue #1, the cited references do not disclose this limitation.

/Steven Chang/
(Applicant/Applicant's Representative) Signature)

(Examiner/SPE Signature)

1. (Proposed Amendment) In a distributed network of interconnected computing devices, a network virus monitor, comprising:

a virus sensor operable in a number of modes arranged to detect a computer virus in the network such that the bandwidth of the network is **minimally affected** ~~**substantially unaffected**~~ in a first mode in that **original** data packets continue to their destination after they are copied creating copied data packets which are analyzed for the computer virus, and wherein when the virus sensor detects the computer virus, the virus sensor switches to a second mode, wherein original data packets are analyzed and a subset of data packets determined to be infected or suspected of being infected are not returned to the network and wherein the virus monitor is able to automatically collect network environment data and assign an IP address to itself, and wherein the virus monitor automatically locates a controller in the network and registers itself with the controller, from where the virus monitor receives a rule set and an outbreak prevention policy (OPP).

6. (Proposed Amendment) A monitor as recited in claim 5, wherein the selected data packets **to be forwarded to the virus monitor** are each associated with the data packet protocol associated with the computer virus ~~**such that only those data packets associated with the identified data packet protocol are selected from the network**~~.

10. (Proposed Amendment) A method of monitoring a distributed network of computing devices for a computer virus at a virus monitor coupled to the distributed network, comprising:

monitoring a flow of data packets in the network for the computer virus without substantially reducing the flow of data packets **in a standby mode**, wherein data packets continue to their destination after they are copied creating copied data packets which are analyzed for the computer virus, thereby preserving network bandwidth ~~**in a standby mode**~~;

determining that at least one of the copied data packets is infected or suspected of being infected with the computer virus;

monitoring the flow of data packets in an inline mode **in response to said determining** wherein original data packets are analyzed and wherein data packets that are determined to be infected or suspected of infection are not returned to the flow of data packets; and

initializing the virus monitor by automatically:

collecting network environment data;

assigning an IP address to the virus monitor;

locating a controller in the network; and

registering the virus monitor with the controller, from where the virus monitor receives a rule set and an outbreak prevention policy.
(OPP).

17. (Proposed Amendment) A computer-readable medium storing computer code for monitoring a distributed network of computing devices for a computer virus at a virus monitor coupled to the distributed network, the computer-readable medium comprising:

computer code for monitoring a flow of data packets in the network for the computer virus without substantially reducing the flow of data packets, wherein data packets continue to their destination after they are copied creating copied data packets which are analyzed for the computer virus, thereby preserving network bandwidth in a standby mode;

computer code for determining that at least one of the copied data packets is infected or suspected of being infected with the computer virus;

computer code for monitoring the flow of data packets in an inline mode **<u>in response to said determining</u>** wherein original data packets are analyzed and wherein data packets that are determined to be infected or suspected of infection are not returned to the flow of data packets;

computer code for automatically collecting network environment data at the virus monitor;

computer code for automatically assigning an IP address to the virus monitor; and

computer code for automatically locating a controller in the network and registering the virus monitor with the controller, from where the virus monitor receives a
rule set and an outbreak prevention policy (OPP).